THE ISOTROPIC PLANE

Prerequisites. Chapter 16, *The invariant derivation at a supersingular prime*: the moments $t(a,w)$, the functions F and Θ and the directions $e_\pm$ of Section 16.1, the formal group $\hat{E}$ and the ring $\mathcal{O}=\mathbb{Z}_p[\mathrm{i}]$ of Section 16.2, the function E_p, Problem 16.3.4 and Theorem 16.4.1, and Section 16.5. Quasi-periods of σ and Legendre's relation [Si2, §I.5]. Decomposition groups in cyclotomic fields. Rational functions and divisors on an abelian scheme over a discrete valuation ring, at the level of the statement that a rational function whose divisor avoids a point is regular there [BK, Lemma 2.13].

17.1. The isotropic plane

The function F does not gain by itself (Problem 16.5.3). Why should Θ along the directions $e_\pm=(1,\pm\zeta)$ do better? They are the eigenlines of an action of $\mathbb{Z}[\zeta]$ on $\mathbb{Z}[\mathrm{i}]^2$. Let

$$\rho(\zeta):=\begin{pmatrix}0&1\\ \mathrm{i}&0\end{pmatrix},$$

let σ_+ be the identity of $\mathbb{Q}(\zeta)$ and σ_- the automorphism $\zeta\mapsto-\zeta$, and let $H(Z,W):=Z_1\bar{W}_1+Z_2\bar{W}_2$.

Problem 17.1.1. ρ extends to a ring homomorphism $\mathbb{Z}[\zeta]\to M_2(\mathbb{Z}[\mathrm{i}])$, and $\rho(\bar{a})=\rho(a)^*$, the conjugate transpose.

Problem 17.1.2. $\rho(a)e_\pm=\sigma_\pm(a)e_\pm$, and $H(e_+,e_-)=0$.

Now let $p\equiv3\pmod 8$. The Frobenius $\zeta\mapsto\zeta^3$ generates the decomposition group of p in $\mathbb{Q}(\zeta)$, with fixed field $\mathbb{Q}(\sqrt{-2})$, $\sqrt{-2}:=\zeta+\zeta^3$. Since $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain, $p=x^2+2y^2$ for integers x, y. We regard $\mathbb{Z}[\zeta]$ as a subring of $\mathcal{O}$.

Problem 17.1.3. After replacing y by $-y$ if necessary, $a:=x+y\sqrt{-2}$ lies in $p\mathcal{O}$, while $\bar{a}=x-y\sqrt{-2}$ is a unit of $\mathcal{O}$. Moreover $\sigma_-(a)=\bar{a}$. (For $p=3$: $a=1\pm\sqrt{-2}$.)

Problem 17.1.4. If $p\equiv7\pmod 8$, then $v_p(a)=v_p(\bar{a})$ for every $a\in\mathbb{Z}[\zeta]$.

Complex conjugation on $\mathbb{Z}[\mathrm{i}]$ reduces modulo p to the Frobenius $z\mapsto z^p$ of $\mathbb{F}_{p^2}$, so H reduces to the hermitian form $h(z,w):=z_1w_1^p+z_2w_2^p$ on $\mathbb{F}_{p^2}^2$. Let $\bar{e}_\pm$ be the reductions of $e_\pm\in\mathcal{O}^2$. The Frobenius sends ζ to ζ^p, which is not $\bar{\zeta}$ when $p\equiv3\pmod 8$; so $h(\bar{e}_+,\bar{e}_-)$ need not vanish although $H(e_+,e_-)=0$.

Problem 17.1.5. $h(\bar{e}_+,\bar{e}_+)=h(\bar{e}_-,\bar{e}_-)=1+\zeta^{p+1}$ and $h(\bar{e}_+,\bar{e}_-)=1-\zeta^{p+1}$. So for $p\equiv3\pmod 8$ both lines are isotropic and h pairs them, while for $p\equiv7\pmod 8$ they are anisotropic and orthogonal.

We call e_- the *partner* of e_+. In terms of embeddings, $\sigma_-=c\circ\mathrm{Frob}\circ\sigma_+$, where c is complex conjugation and $\mathrm{Frob}(\zeta)=\zeta^p$; for $p\equiv7\pmod 8$, by contrast, $c\circ\mathrm{Frob}\circ\sigma_+=\sigma_+$. The derivatives along e_+ will gain, and those along the partner e_- will pay for it.

Date: November 24, 2026.

17.2. Integrality on an eigenline

Let $P(s) := \Theta(se_+) = F(s)\,F(\zeta s)$. Since F is even, $\Theta(te_-) = P(t)$, and $t(n,0) = P^{(n)}(0)$. Write $P(s) = \hat{P}(\operatorname{sl} s)$ with $\hat{P} \in \mathbb{Q}[[X]]$. We show that $\hat{P}$ is p-integral, unlike F.

Let L be the period lattice of sl and η the quasi-period map of Λ. Since $\eta(\mathrm{i}\omega) = -\mathrm{i}\eta(\omega)$, Legendre's relation gives $\eta(\omega) = (\pi/\operatorname{vol}\Lambda)\,\bar{\omega}$, and with the law $\sigma(u+\omega) = \pm e^{\eta(\omega)(u+\omega/2)}\sigma(u)$ [Si2, §I.5],

$$F(u+\omega) = \exp\bigl(c\,\bar{\omega}u + \tfrac{c}{2}|\omega|^2\bigr)F(u), \qquad \omega \in \Lambda, \quad c := \frac{2\pi}{\operatorname{vol}\Lambda}.$$

Problem 17.2.1. For $\gamma \in L^2$, $\Theta(Z+\gamma) = \exp\bigl(cH(Z,\gamma) + \frac{c}{2}H(\gamma,\gamma)\bigr)\Theta(Z)$. For $a \in \mathbb{Z}[\zeta]$, $a \neq 0$, the function

$$F_a(Z) := \frac{\Theta(\rho(a)Z)}{\Theta(\rho(\bar{a})Z)}$$

is L^2-periodic with $F_a(0) = 1$, hence a rational function on $E \times E$.

Problem 17.2.2. On $\mathbb{C}/L = E(\mathbb{C})$, the zeros of F are the two points at infinity of $y^2 = 1 - X^4$, each with multiplicity two.

Let $\mathcal{A}$ be $E \times E$ over $\mathcal{O}$, an abelian scheme on which $\mathbb{Z}[\zeta]$ acts through ρ, and write $\hat{F}_a(X_1, X_2)$ for the expansion of F_a in $X_1 = \operatorname{sl} Z_1$, $X_2 = \operatorname{sl} Z_2$.

Problem 17.2.3. $\hat{F}_a \in \mathcal{O}[[X_1, X_2]]$.

Now let $p \equiv 3 \pmod 8$, and let a be as in Problem 17.1.3.

Problem 17.2.4. $\hat{P}([a]X) = \hat{F}_a(X, [\zeta]X)\,\hat{P}([\bar{a}]X)$.

Problem 17.2.5. The coefficients of $\hat{P}$ lie in $\mathbb{Z}_{(p)}$.

Problems 17.2.1–17.2.5 and Theorem 16.4.1 prove the following.

Theorem 17.2.1. *Let $p \equiv 3 \pmod 8$. Then $\hat{P} \in \mathbb{Z}_{(p)}[[X]]$, and $v_p(t(n,0)) = v_p(P^{(n)}(0)) \geq E_p(n)$ for every $n \geq 0$.*

The induction in Problem 17.2.5 is the argument Bannai and Kobayashi use for the Kronecker theta function at ordinary primes [BK, Prop. 2.14], where one element of the CM order serves for all coordinates at once. Here $\mathcal{A}$ is supersingular, but on the line $\mathbb{C}e_+$ the element a acts by a non-unit and $\bar{a}$ by a unit. At $p \equiv 7 \pmod 8$ there is no such element (Problem 17.1.4), and at $p = 7$ the conclusion fails.

Problem 17.2.6. $\hat{P}(X) = 1 - \frac{1}{70}X^8 + O(X^{12})$. So $\hat{P}$ is not 7-integral, and $t(8,0) = -576$.

17.3. The cross term

Theorem 17.2.1 accounts for the derivatives along each axis. What remains is a factor equal to 1 on both axes. Throughout, $p \equiv 3 \pmod 8$, $X_1 = \operatorname{sl} s$, $X_2 = \operatorname{sl} t$, and $P_n := P^{(n)}(0)$.

Problem 17.3.1. $J(s,t) := \partial_s\partial_t \log\Theta(se_+ + te_-) = 2\operatorname{sl}^2(s+t) - 2\mathrm{i}\,\operatorname{sl}^2\bigl(\zeta(s-t)\bigr)$, and $J \in \mathcal{O}[[X_1, X_2]]$.

Let $M(s,t) := \int_0^s \int_0^t J$, and $M_{\alpha\beta} := \partial_s^\alpha \partial_t^\beta M(0,0)$.

Problem 17.3.2. $\Theta(se_+ + te_-) = P(s)\,P(t)\,e^{M(s,t)}$. The numbers $M_{\alpha\beta}$ vanish unless $\alpha, \beta \geq 1$, and then $M_{\alpha\beta} \in p^{E_p(\alpha-1)}\mathcal{O}$.

Problem 17.3.3. Let S and T be sets with a and w elements. Then

$$t(a,w) = \sum P_{|S_0|}\,P_{|T_0|} \prod_{B\in\pi} M_{|B\cap S|,|B\cap T|},$$

the sum over subsets $S_0 \subseteq S$, $T_0 \subseteq T$, and partitions π of $(S \smallsetminus S_0) \sqcup (T \smallsetminus T_0)$ into blocks each meeting both S and T.

Problem 17.3.4. Each term in Problem 17.3.3 has at most w blocks and valuation at least $\lfloor a/p \rfloor - w$.

So $v_p(t(a,w)) \geq \lfloor a/p \rfloor - w$. For the higher odd levels one must also use the multiplicities of the terms. Group the terms of Problem 17.3.3 by $a_0 = |S_0|$, $w_0 = |T_0|$, and the number $m_{\alpha\beta}$ of blocks with $|B\cap S| = \alpha$ and $|B \cap T| = \beta$.

Problem 17.3.5. The number of terms with given a_0, w_0 and $(m_{\alpha\beta})$ is $N \cdot a!/\big(a_0! \prod_{\alpha,\beta} (\alpha!)^{m_{\alpha\beta}}\big)$ with N a positive integer.

Problem 17.3.6. Let $\alpha_1, \ldots, \alpha_k \geq 1$ and $a_0 \geq 0$ have sum a, and let $n_i := \#\{b : p^i \mid \alpha_b\}$. Then

$$v_p\Big(\frac{a!}{a_0!\,\alpha_1!\cdots\alpha_k!}\Big) + E_p(a_0) + \sum_{b=1}^{k} E_p(\alpha_b - 1) \;\geq\; \sum_{\substack{i\geq 1\\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - n_i\Big)_+,$$

where $x_+ := \max(x, 0)$.

Since $n_i \leq k \leq w$, Problems 17.3.2–17.3.6 and Theorem 17.2.1 bound every group of terms. With the symmetry $t(a,w) = t(w,a)$ of Problem 16.1.5, this proves the following.

Theorem 17.3.1. *Let $p \equiv 3 \pmod 8$. For all integers $a, w \geq 0$,*

$$v_p\big(t(a,w)\big) \;\geq\; \max\left(\sum_{\substack{i\geq 1\\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - w\Big)_+,\; \sum_{\substack{i\geq 1\\ i \text{ odd}}} \Big(\Big\lfloor \frac{w}{p^i} \Big\rfloor - a\Big)_+ \right).$$

In the table of Section 16.1 the bound is an equality whenever it is positive. It is not always sharp: $t(11,1) = -2^9 \cdot 3^6$, while the bound at $p = 3$ is 2.

Exercise. If $M = s^p t/p$, then $\partial_s^{pw} \partial_t^w e^M(0) = (pw)!/p^w$, of valuation $v_p(w!)$. For $w < p$ this is 0, whereas a series integral in X_1, X_2 would give at least w by Problem 16.3.4: each block $s^p t/p$ loses one factor of p.

17.4. Questions

Theorem 17.3.1 does not extend to $p \equiv 7 \pmod 8$: it fails at $p = 7$ (Problem 17.2.6). What fails is the choice of directions: $e_\pm$ are global eigenlines of $\mathbb{Z}[\zeta]$, and they are isotropic modulo p only for $p \equiv 3 \pmod 8$ (Problem 17.1.5). For every $p \equiv 3 \pmod 4$, the form H on $\mathcal{O}^2$ has a basis f, f' with $H(f,f) = H(f',f') = 0$ and $H(f,f') = 1$, which need not come from any element of the CM order. Adriazola [Adr, §8.6 and Thm. 8.21] writes theta functions of hermitian lattices in such local

hyperbolic coordinates over $\mathbb{Z}_{p^2}$, using the action of all of $\mathbb{Z}_{p^2}$ on the formal group [Adr, Lemma 8.13], and obtains the gain at the odd levels at every inert $p \geq 5$, for the imaginary quadratic fields used there, with no condition modulo 8 [Adr, Thm. 11.45]. That result assumes that the constant in the kernel law is integral; in [Adr] this is [Adr, Hyp. 11.42, (N3)]; see the ledger in Section 58.7 of Chapter 58. The Lean formalization [Lean] does not assume it: it proves an integral kernel law of this shape for the kernels it uses, by a different route, in which the exponent is a torus average of a coboundary of the logarithm of the sigma function of one CM curve, and the integrality comes from a factorization of the fourth tensor power of the kernel into sigma functions. So the restriction $p \equiv 3 \pmod 8$ belongs to the eigenline model of this chapter, not to the argument.

Let A be an abelian variety with complex multiplication by the ring of integers of a CM field K, with CM type Φ, and let Θ be a normalized theta function on its universal cover. The eigenlines $\mathbb{C}e_\phi$ ($\phi \in \Phi$) replace $e_\pm$; the case above is $K = \mathbb{Q}(\zeta)$, $\Phi = \{\sigma_+, \sigma_-\}$. The argument of Section 17.2 on $\mathbb{C}e_\phi$ needs an element a of the CM order with $\phi(a)$ a non-unit and $\phi(\bar{a})$ a unit, and such an element exists exactly when complex conjugation does not fix the prime of K determined by ϕ. Theorem 17.3.1 subtracts at each odd level i the order of differentiation along $c \circ \mathrm{Frob}^i \circ \sigma_+ = \sigma_-$. We do not know whether in general the weight subtracted at level i from the order along e_ϕ is the order along $c \circ \mathrm{Frob}^i \circ \phi$, at the levels with $\mathrm{Frob}^i \circ \phi \notin \Phi$.

For $E \times E$ the eigenline argument fails only at $p \equiv 7 \pmod 8$, and there the hyperbolic coordinates above are the way around it. The eigenline argument fails at every supersingular prime for the Jacobian of $y^2 = x^5 - 1$, with CM by $\mathbb{Q}(\zeta_5)$. For odd $p \not\equiv 0, 1 \pmod 5$, complex conjugation lies in the decomposition group of every prime above p, and these are the primes at which the Jacobian is supersingular. We do not know whether the restriction of Θ to an eigenline is p-integral in the formal parameter at these primes, nor what lower bound holds for its derivatives at the origin.

Hints

§17.1.

17.1.1: $\rho(\zeta)^2 = \mathrm{i}$, and $\rho(\zeta)$ is unitary.

17.1.3: $a\bar{a} = p$, and $\mathcal{O}$ is a discrete valuation ring with uniformizer p.

17.1.4: The Frobenius automorphism of $\mathcal{O}$ preserves v_p and maps ζ to ζ^p.

§17.2.

17.2.1: $\rho(a)$ preserves L^2 because $\mathrm{i}L = L$, and $\rho(a)^*\rho(a) = \rho(a\bar{a}) = \rho(\bar{a})^*\rho(\bar{a})$.

17.2.2: $F = \sigma^2/\,\mathrm{sl}^2$ by Problem 16.1.1.

17.2.3: The Taylor coefficients of F_a lie in $\mathbb{Q}(\mathrm{i})$, so F_a is a rational function on $E \times E$ over $\mathbb{Q}(\mathrm{i})$. Find its divisor on $\mathcal{A}$ near the origin of the special fiber, using Problem 17.2.2 and the fact that the points at infinity of E do not meet the origin modulo p. Since a divides the nonzero integer $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a)$ in $\mathbb{Z}[\zeta]$, both $\rho(a)$ and $\rho(\bar{a})$ are isogenies on the special fiber, so pulling back the closure of the zero divisor of Θ adds no vertical component. The condition $F_a(0) = 1$ excludes the special fiber itself.

17.2.4: Evaluate $\Theta(\rho(a)Z) = F_a(Z)\Theta(\rho(\bar{a})Z)$ at $Z = se_+$, using Problems 17.1.2 and 16.2.4.

17.2.5: Induction on the degree, comparing coefficients of X^n in Problem 17.2.4.

§17.3.

17.3.1: Problem 16.5.1. Then $\mathrm{sl}(s+t) = X_1 \oplus X_2$ and $\mathrm{sl}(\zeta(s-t)) = [\zeta](X_1 \ominus X_2)$.

17.3.2: Restrict $\log \Theta$ to the two axes. For the bound, express $M_{\alpha\beta}$ through derivatives of J, and use Theorem 16.4.1.

17.3.3: Expand $e^M = \sum_k M^k/k!$ and distribute the $a+w$ labelled derivatives.

17.3.4: Each block meets T. Keep only the first level of each E_p.

17.3.5: Choose the T-parts first; after that the blocks are distinguishable.

17.3.6: Apply Legendre's formula level by level, and use $\lfloor \alpha/p^i \rfloor - \lfloor (\alpha - 1)/p^i \rfloor \in \{0, 1\}$. Each level contributes a nonnegative amount.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[BK] K. Bannai and S. Kobayashi, *Algebraic theta functions and the p-adic interpolation of Eisenstein–Kronecker numbers*, Duke Math. J. **153** (2010), 229–295; arXiv:math/0610163. Numbering as in the arXiv version.

[Lean] The Lean community, *riemann-hypothesis*, a Lean formalization of Alpöge's argument, `https://github.com/leanprover-community/riemann-hypothesis`.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.